WHAT IS CLAIMED IS:

1. An authentication method comprising the steps of:

generating a first security context in response to a first user authentication;

generating a second security context in response to a second user authentication, wherein said second security context aggregates said first security context and a security context corresponding to an identity in said second user authentication.

2. The method of claim 1 further comprising the step of saving said first security context.

3. The method of claim 2 wherein said step of saving said first security context comprises the step of pushing said first security context on a stack.

4. The method of claim 1 further comprising the step of receiving a user logoff.

5. The method of claim 4 further comprising the step of destroying said second security context in response to said step of receiving said user logoff.

6. The method of claim 2 further comprising the step of reverting to said first security context in response to a user logoff.

7. The method of claim 6 wherein said step of reverting to said first security context

comprises the step of popping said first security context off of a stack.

8. The method of claim 1 further comprising the step of determining an access permission in response to said second security context.

9. A computer program product embodied in a tangible storage medium, the program product comprising a program of instructions for performing the method steps of:

generating a first security context in response to a first user authentication;

generating a second security context in response to a second user authentication, wherein said second security context aggregates said first security context and a security context corresponding to an identity in said second user authentication.

10. The program product of claim 9 further comprising instructions for performing the step of saving said first security context.

11. The program product of claim 10 wherein said step of saving said first security context comprises the step of pushing said first security context on a stack.

12. The program product of claim 9 further comprising instructions for performing the step of receiving a user logoff.

13. The program product of claim 12 further comprising instructions for performing the step of destroying said second security context in response to said step of receiving said user logoff.

14. The program product of claim 10 further comprising instructions for performing the step of reverting to said first security context in response to a user logoff.

15. The program product of claim 14 wherein said step of reverting to said first security context comprises the step of popping said first security context off of a stack.

16. The program product of claim 9 further comprising instructions for performing the step of determining an access permission in response to said second security context.

17. A data processing system comprising:

circuitry operable for generating a first security context in response to a first user authentication;

circuitry operable for generating a second security context in response to a second user authentication, wherein said second security context aggregates said first security context and a security context corresponding to an identity in said second user authentication.

18. The system of claim 17 further comprising circuitry operable for saving said first security context.

19. The system of claim 18 wherein said circuitry operable for saving said first security context comprises the step of pushing said first security context on a stack.

20. The system of claim 17 further comprising circuitry operable for receiving a user logoff.

21. The system of claim 20 further comprising circuitry operable for destroying said second security context in response to said step of receiving said user logoff.

22. The system of claim 18 further comprising circuitry operable for reverting to said first security context in response to a user logoff.

23. The system of claim 22 wherein said circuitry operable for reverting to said first security context comprises circuitry operable for popping said first security context off of a stack.

24. The system of claim 17 further comprising circuitry operable for determining an access permission in response to said second security context.